Quantum Information Processing (2020) 19:134
https://doi.org/10.1007/s11128-020-02632-6

Coding in the entanglement domain

Marius Nagy[1,3] · **Naya Nagy**[2]

Received: 10 March 2019 / Accepted: 5 March 2020 / Published online: 12 March 2020

Abstract
Moving at the speed of light, the photon is the ideal physical support to transmit information. Polarization of a photon is the predominant quantum property used to encode information, but other encoding domains, such as the spatial-mode degree of freedom, have been considered. In this paper, we put forward the entanglement degree of freedom of a photon as an exploitable resource for encoding information in quantum cryptographic protocols. We show how classical information can be extracted from the quantum state of a photon by distinguishing between a singular, independent state and an entangled state through interferometry. We also give a direct application of our technique to quantum key distribution as a proof of concept for future quantum protocols that may use coding in the entanglement domain in combination with other degrees of freedom that are currently exploited for cryptographic purposes.

Keywords Quantum cryptography · Entanglement · Interferometry · Quantum key distribution

1 Introduction

With the advent of quantum information processing, researchers have considered different ways to encode information using quantum properties of elementary particles. For the purpose of quantum computation, the qubits composing the quantum computer are *static*, in the sense that they occupy a clearly delimited region of space, regardless

✉ Marius Nagy
mnagy@pmu.edu.sa; marius@cs.queensu.ca

Naya Nagy
nmnagy@iau.edu.sa

1 College of Computer Engineering and Science, Cybersecurity Center, Prince Mohammad Bin Fahd University, Al Azeziya, Eastern Province, Kingdom of Saudi Arabia

2 College of Computer Science and IT, Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia

3 School of Computing, Queen's University, Kingston, ON, Canada

of the particular physical realization of a qubit (nuclear magnetic resonance, Josephson junctions, quantum dots or trapped ions) [8,16]. In quantum cryptography, however, information usually has to be transmitted between communicating parties, so it was clear from the very beginning that photons are the ideal candidates to implement *flying qubits*. And since *polarization* is the most flexible and easy to manipulate quantum property of a photon, virtually all quantum cryptograhic schemes, from the seminal paper that started the field in 1984 [3] to recent advances [1,15,18,20], they all employ photons and their polarization.

As these quantum cryptographic protocols developed and improved over time, both in terms of security as well as efficiency, people started looking for multiple ways of encoding information in the quantum state of a photon. Alongside this direction, harnessing spatial-mode degrees of freedom for a photon seems to be a very promising idea for increasing the efficiency of quantum key distribution protocols, due to the potentially high information capacity per photon [15]. Different schemes have been proposed to double the capacity of the transmission channel in multi-party key agreement protocols by combining photon polarization with a simple way to encode a bit into the spatial-mode degree of freedom brought about by the use of a beam splitter [1,20]. Other researchers have shown how a higher dimensionality can be achieved by controlling the radial degree of freedom of a photon's spatial mode [15] or by structuring the spin and orbital angular momentum of light [18].

Encoding a bit of information in any degree of freedom of a photon requires an orthonormal basis to be defined in the state space spanned by that particular degree of freedom. Furthermore, entanglement can then be defined between two photons, if their quantum properties corresponding to that particular degree of freedom (such as polarization, for example) are always correlated, regardless of the particular measurement basis employed. However, none of the schemes mentioned above considers entanglement itself as a possible encoding domain. In this paper, we explore exactly this option of encoding information in the fact that a photon may or may not be entangled with another one. The type of entanglement harnessed for our purpose is spatial entanglement, and we show herein how information encoded in the entanglement domain can be extracted from a photon by relying on its interference properties.

The main contribution of this paper is a proof of concept that the quantum state of a photon as being spatially entangled or not constitutes an encoding domain that can be exploited for cryptographic purposes. We describe a possible QKD scheme using only the entanglement domain to encode information, but we envisage that future cryptographic protocols may combine the entanglement domain with other degrees of freedom of a photon to create more efficient, multiplexed schemes. Along this direction, we briefly discuss how our QKD scheme may be combined with the BB84 protocol in order to increase its efficiency in terms of the amount of information transmitted per photon. The remainder of the paper is structured as follows. In the next section, we provide a detailed exposition on the distinguishability of a spatially entangled photon through interferometry. Section 3 investigates the capacity of a communication channel that is used to transmit information encoded in the entanglement domain. A quantum key distribution protocol designed to exploit our entanglement encoding scheme together with an extension that also uses polarization as an additional encoding domain are presented in Sect. 4. Section 5 explores some

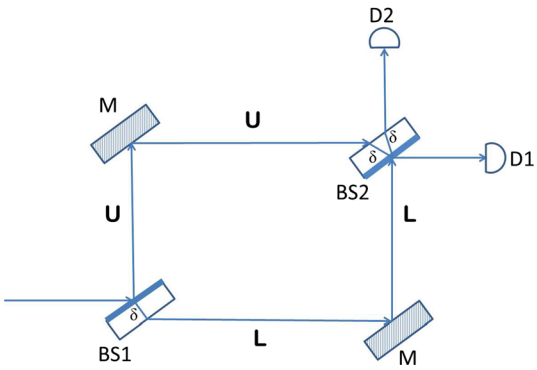

Fig. 1 Mach–Zehnder interferometer

of the ramifications of encoding in the entanglement domain into the impossibility of quantum bit commitment and superluminal communication. Finally, conclusions are offered in Sect. 6.

2 Verifying entanglement through interferometry

In this section, we provide a detailed explanation of how an entangled photon can be distinguished from a non-entangled one through the use of an interferometer. The particular type of interferometer used is less important since the basic idea allowing us to distinguish between entanglement and non-entanglement is that the quantum state of an entangled pair of photons can be described mathematically in a similar way to the entanglement between a photon and the measuring device acting on it, thus making entanglement behave as a sort of measurement and destroying any possible interference set up by the experimental apparatus.

The Mach–Zehnder interferometer [6], depicted in Fig. 1, is composed of two beam splitters and two mirrors. A beam splitter is a "half-silvered" mirror that reflects half the light incident on it and refracts the other half. When a single photon arrives at the beam splitter, its quantum state becomes a superposition of being both reflected and refracted, such that the photon travels through both the upper and the lower arms of the interferometer simultaneously. This allows the photon to interfere with itself at the second beam splitter and always exit the interferometer through the same branch and be detected by the same photon detector. We will now prove formally that any photon that enters the experimental setup horizontally (as shown in the figure) will always leave the interferometer horizontally and consequently, will trigger photon detector $D1$.

The effect of each beam splitter and mirror on a traveling photon can be described as a quantum operator acting on the state space spanned by the two basis vectors:

$$|L\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |U\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1}$$

$|L\rangle$ identifies the basis state in which a photon travels through the lower arm of the interferometer, while $|U\rangle$ labels the state that corresponds to a photon traveling through the upper arm. In order to define the quantum operator assimilated with a beam splitter, we have to consider the following facts. When a light beam is incident on a surface and the material on the other side of the surface has a higher index of refraction than the medium that the light is traveling from, then the reflected light beam is shifted in its phase by exactly one half a wavelength. This means that the quantum state of the reflected photon picks up a phase of $e^{i\pi} = -1$. This happens when a photon that enters the interferometer horizontally is reflected by the first beam splitter.

On the other hand, when a light beam is incident on a surface and the material on the other side of the surface has a lower index of refraction than the medium that the light is traveling from, then the reflected light beam does not have its phase changed. This happens when a photon enters the interferometer vertically, and it is reflected by the reflective surface of $BS1$. However, before hitting the reflective surface of the beam splitter, the photon must travel through the material from which the beam splitter is constructed (usually, some kind of glass). In doing so, the quantum state of the photon again picks up a phase that depends on the index of refraction of that respective material and the optical path length δ covered by the photon through the material.

Finally, when a light beam is refracted at the surface separating two mediums, its direction changes, but its phase is not affected. Based on these observations, we can now provide a full description of the effect the first beam splitter would have on a horizontally/vertically incident photon:

$$BS1 = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{2i\theta} & e^{i\theta} \\ e^{i\theta} & -1 \end{pmatrix}. \tag{2}$$

The above matrix description of $BS1$ tells us that the quantum state of a photon traveling toward the beam splitter vertically, from below, would be simultaneously reflected into the lower arm and refracted through the beam splitter medium into the upper arm. Each component would have its phase changed, according to the optical distance covered: the refracted beam travels distance δ through the beam splitter material and in the process acquires a certain phase shift θ, while the reflected beam covers twice that distance, since it takes distance δ just to reach the reflective surface of $BS1$ and then another δ to exit the beam splitter through the lower arm. Consequently, the phase shift acquired by the lower arm component is 2θ.

However, in our experimental setup, the photon enters the interferometer horizontally. The fate of such a photon is described by the second column in the matrix. Its quantum state becomes a balanced superposition of the photon being reflected to the upper arm (with a phase shift of π) and traveling through the beam splitter in the lower arm (in which case it acquires a phase shift of θ to account for the path δ covered by the photon through the material from which the beam splitter is made up).

The second beam splitter acts as a similar quantum operator, with the first column in its matrix description showing the effect of $BS2$ on a photon coming toward it from the lower arm and the second column revealing what would happen to a photon arriving at $BS2$ from the upper arm:

$$BS2 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & e^{i\theta} \\ e^{i\theta} & e^{2i\theta} \end{pmatrix}. \tag{3}$$

Unlike $BS1$, the second beam splitter is placed with its reflective surface facing down, so a photon reaching $BS2$ from the lower arm of the interferometer is reflected directly (without traveling through the beam splitter's material) as opposed to the refracted beam, which has to cover the distance δ through the medium from which the beam splitter is fabricated. This explains why the reflected beam has its phase shifted by half a wavelength ($e^{i\pi} = -1$), while the phase shift of θ acquired by the refracted beam corresponds to the optical distance δ covered through the medium of the beam splitter.

In the case of a photon incident on $BS2$ horizontally (from the upper arm), both the reflected and the refracted beams have to travel distance δ to reach the reflective (or, to be more precise, half-reflective) surface of the beam splitter. Since the reflected beam has to go through another δ in order to exit the beam splitter vertically (upper arm), the phase shift of the reflected beam (corresponding to the $|U\rangle$ component or base vector) is double the phase change of the refracted beam (which corresponds to base vector $|L\rangle$).

Finally, we are left with describing the effect of the two mirrors on the two base vectors spanning the state space of a photon traveling through the interferometer. Regardless of the particular arm we focus on, the effect is the same: the beam is directly reflected by the surface separating the mirror's material from air and, consequently, has its phase changed by π:

$$M = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4}$$

We now have all the required elements to formally describe the quantum state of a photon that enters the interferometer horizontally and travels through the two arms of the apparatus. The initial quantum state of such a photon is simply $|U\rangle$ (any photon incident on a beam splitter horizontally is described by base vector $|U\rangle$, while a photon exiting a beam splitter horizontally is described by base vector $|L\rangle$). Then, the photon goes through the first beam splitter $BS1$ and is reflected by the mirror M in order to converge on the second beam splitter $BS2$. Therefore, its final quantum state is:

$$BS2 \cdot M \cdot BS1|U\rangle = \frac{1}{2} \begin{pmatrix} 2e^{i\theta} \\ 0 \end{pmatrix} = e^{i\theta}|L\rangle. \tag{5}$$

Since the only component present in this final state is $|L\rangle$, it is guaranteed that the photon will always leave the interferometer horizontally, causing detector $D1$ to register a hit. The global phase of θ corresponds to the phase shift triggered by the photon traveling the optical distance δ through the beam splitter medium, in its way from the entry point ($BS1$) to the exit point ($BS2$). Note that the same distance δ is traveled by both the lower arm component, as well as the upper arm component, such that when they reunite at $BS2$, they create a global phase of θ.

The mathematical details presented above clearly demonstrate that the horizontal component exiting the interferometer is reinforced through interference, while the vertical component is destroyed through the same phenomenon. Intuitively, since there

is only one photon at any given time in the experimental apparatus, the photon interferes with itself, or to be more precise, the lower arm component interferes with the upper arm component. This interference is possible as long as we have no information, not even the theoretical possibility of obtaining such information, about which way the photon traveled through the interferometer. We show next that if an entangled photon enters a Mach–Zehnder interferometer, no interference takes place between the two arms of the apparatus, exactly because it is possible to obtain the "which way" information from the other photon in the entangled pair.

The standard method for obtaining pairs of entangled photons nowadays is the nonlinear optical process of *spontaneous parametric down conversion* (SPDC) [11], in which photons from a pump laser beam, within a nonlinear crystal, can spontaneously be converted into pairs that are momentum and frequency entangled. However, there are two variants of this process. In type-I SPDC, a signal and an idler photons with parallel polarizations are symmetrically emitted along the surface of a cone. In a type-II SPDC experiment, on the other hand, the two photons have trajectories that are constrained along the edges of two cones, whose axes are symmetrically arranged relative to the pump beam and have polarizations perpendicular to each other.

Suppose now that we have obtained a pair of entangled photons through SPDC and we direct each photon in the pair toward a Mach–Zehnder interferometer of its own. Depending on the particular type of entanglement generation employed, we assume the following modifications to the standard Mach–Zehnder interferometer described above and depicted in Fig. 1. If the entangled photons are obtained through type-I SPDC, a double-slit or a double-aperture configuration is used instead of the first beam splitter of the interferometer to create a fork in the photon's path. Such experimental setups are described and analyzed rigorously in [10,17]. The conjugating properties of the entangled pair always force one photon to take the upper path and the other photon to take the lower path.

If the photons are emitted through a type-II SPDC, then the separation between the upper arm and the lower arm of the interferometer can easily be achieved using a polarizer beam splitter, which ensures that, if measured, one photon will always be found in the upper arm of its interferometer, while the other photon will surely be detected in the lower arm. This is due to the fact that in type-II SPDC the entangled photons have always perpendicular polarizations. Consequently, the state of a single pair of photons in the ensemble after going through $BS1$ is:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|L_1\rangle|U_2\rangle + |U_1\rangle|L_2\rangle), \tag{6}$$

where the index 1 in $|L_1\rangle$ and $|U_1\rangle$ denotes the state space of the first particle in the pair (going through interferometer 1) and index 2 denotes the state space of the second particle, going through interferometer 2. Note that, if a polarizer beam splitter is used, then the two arms of the interferometer will have perpendicular polarizations, and therefore, an additional polarization rotator has to be inserted into one of the two arms to restore the indistinguishability of the two paths and allow for the interference at the second beam splitter to take place.

As the analysis in [17] clearly shows, the quantum state describing the path (momentum) entangled pair of photons obtained through type-I SPDC, after passing through the two slits, is a Bell-like state similar to Eq. 6. Therefore, regardless of how the upper and lower paths are created (either using a type-I SPDC with double apertures playing the role of $BS1$ or a type-II SPDC where $BS1$ is a polarizer beam splitter), the net effect is a path-entangled pair of photons, whose spatial locations are accurately described by Eq. 6 or an equivalent one up to a relative phase.

This same state also characterizes the entangled pair after being reflected by the mirrors in both interferometers, since each of the four base vectors, $|L_1\rangle$, $|L_2\rangle$, $|U_1\rangle$ and $|U_2\rangle$ picks up a phase shift of $e^{i\pi} = -1$ due to the reflection. Finally, applying the operator $BS2$ on each of the two photons, we obtain the state of the ensemble as it leaves the two interferometers:

$$\frac{1}{\sqrt{2}}\left(\frac{-|L_1\rangle + e^{i\theta}|U_1\rangle}{\sqrt{2}} \cdot \frac{e^{i\theta}|L_2\rangle + e^{2i\theta}|U_2\rangle}{\sqrt{2}} + \frac{e^{i\theta}|L_1\rangle + e^{2i\theta}|U_1\rangle}{\sqrt{2}} \cdot \frac{-|L_2\rangle + e^{i\theta}|U_2\rangle}{\sqrt{2}}\right)$$
$$= -\frac{e^{i\theta}}{\sqrt{2}}(|L_1L_2\rangle - e^{2i\theta}|U_1U_2\rangle). \tag{7}$$

The balanced superposition that characterizes this final state shows that a photon can exit its interferometer either through the upper arm or through the lower arm, with equal probability and furthermore, the outcomes are always correlated, due to the entanglement.

Note that the same behavior for photon 1 would be obtained even if photon 2 is not forced through any experimental apparatus. State $|\psi_1\rangle$ from Eq. 6 would still describe the ensemble of entangled photons in that case, telling us that if we were to measure the position of photon 1 and found it to be in the lower arm, then photon 2 would certainly be detected in the upper arm, if we were to run it through an interferometer. Similarly, if we know that photon 1 travels through the upper arm of its interferometer, then for sure photon 2 would be detected traveling the lower arm, if subjected to an interferometer.

The fact that the $|L_1\rangle$ and $|U_1\rangle$ components in Eq. 6 are "tagged" with hypothetical states of photon 2 makes the interference between the two arms at $BS2$ impossible, or in other words, entanglement destroys interference. Formally, applying quantum operators M and then $BS2$ just to photon 1 amounts to:

$$\begin{aligned} BS2 \cdot M|\psi_1\rangle &= -\frac{1}{2}(-|L_1\rangle + e^{i\theta}|U_1\rangle) \otimes |U_2\rangle + (e^{i\theta}|L_1\rangle + e^{2i\theta}|U_1\rangle) \otimes |L_2\rangle) \\ &= -\frac{1}{2}(-|L_1\rangle|U_2\rangle + e^{i\theta}|U_1\rangle|U_2\rangle + e^{i\theta}|L_1\rangle|L_2\rangle + e^{2i\theta}|U_1\rangle|L_2\rangle). \end{aligned} \tag{8}$$

As there is no cancelation of terms due to interference, photon 1 has an equal chance of being detected as exiting the interferometer horizontally or vertically. However, in this case, there is no correlation between the final states of the two photons in the pair because the second photon was not manipulated in any way.

Equation 5 on one hand and Eqs. 7 and 8 on the other hand, clearly show that a Mach–Zehnder interferometer can achieve some distinguishability between an entangled photon and a non-entangled photon entering it. Since a non-entangled photon always exits horizontally (according to Eq. 5) and a photon part of an entanglement can exit either horizontally or vertically with equal probability (according to Eq. 7 and 8), it follows that an entangled photon has a 50% chance to be distinguished from an unentangled photon. The distinguishability is achieved when the photon exits the interferometer through the upper arm and is detected by photon detector $D2$.

3 Capacity of a channel using entanglement domain coding

The scheme detailed in the previous section for telling apart an entangled photon from a non-entangled one can be used to transmit information between two parties, with the photon acting as physical support for the information transmitted. If a spatially entangled photon could be reliably distinguished (that is, 100% of the time) from a non-entangled one, then we would be able to transmit one bit of information for each photon traveling from source to destination. Since the Mach–Zehnder interferometer does not achieve a full separation between entangled and non-entangled photons, we analyze in this section the amount of information transmitted or, in other words, the capacity of a channel using spatial entanglement as the domain to encode information.

Suppose, for concreteness, that Alice wants to send information to Bob by encoding it in the entanglement domain: In order to send a bit 0, she generates a pair of spatially entangled photons (as detailed in Sect. 2) and sends photon 1 toward Bob, while keeping its pair, photon 2, for herself; to send a bit 1, she generates and sends a single photon to Bob. When Bob receives the photon from Alice, he runs it through a Mach–Zehnder interferometer and observes the result. The Mach–Zehnder interferometer acts as a measuring device with the two possible outcomes: photon exiting vertically and triggering detector $D2$, respectively, the photon exiting horizontally and ending up in detector $D1$. When $D2$ detects a photon, we know that photon is part of an entangled pair and therefore must encode a 0. However, assuming that the probabilities of receiving a 0 (entangled photon) and a 1 (non-entangled photon) are equal, the event of $D2$ triggering occurs only 25% of the time. In the remaining 75% of the time, detector $D1$ triggers, but in that case, we cannot tell with certainty what the photon encodes: it could still be an entangled photon (in one out of three cases) or a non-entangled photon, that always exits horizontally (in two out of three cases). Consequently, the amount of information carried by a single photon is:

$$\frac{1}{4}\cdot 1+\frac{3}{4}\left(1-\left(-\frac{1}{3}\log\frac{1}{3}-\frac{2}{3}\log\frac{2}{3}\right)\right)=\frac{1}{4}+\frac{3}{4}\left(1+\frac{2}{3}-\log 3\right)\approx 0.31 \quad (9)$$

In order to increase the amount of information sent to Bob close to one bit, Alice needs to repeat the procedure several times. To be more precise, if Alice's intention is to transmit a 0, she generates n pairs of spatially entangled photons and sends one photon from each pair to Bob. Alternatively, if she intends to transmit a 1, then she sends n unentangled photons. With every additional photon sent, the amount of

Fig. 2 Graph quantifying the relationship between the number of photons transmitted and the amount of information carried

information sent to Bob gets closer to one bit. Thus, for two photons transmitted, the amount of information carried is:

$$\frac{3}{8}\cdot 1+\frac{5}{8}\left(1-\left(-\frac{1}{5}\log\frac{1}{5}-\frac{4}{5}\log\frac{4}{5}\right)\right)=1+\frac{5}{8}\left(\frac{8}{5}-\log 5\right)\approx 0.55 \quad (10)$$

This is due to the fact that for two photons, there are four possible outcomes (both exit horizontally, both vertically, one horizontally and one vertically) and in three of these cases, when at least one photon exits vertically, we know with certainty that the bit transmitted is 0, since only an entangled photon can trigger detector $D2$. When both photons exit horizontally (event that happens with probability $5/8$), there is some uncertainty about the bit encoded in the two photons because there is still a $1/5$ probability that the two photons are each part of an entangled pair and they both exited the interferometer horizontally by chance.

In general, if Alice sends a group of n photons that encode either a 0 or a 1, the amount of information transmitted becomes:

$$\frac{2^n-1}{2^{n+1}}+\frac{2^n+1}{2^{n+1}}\left(1+\frac{2^n}{2^n+1}\cdot n-\log\left(2^n+1\right)\right)=\frac{n+1}{2}-\frac{\log\left(2^n+1\right)}{2^{n+1}}. \quad (11)$$

Figure 2 illustrates exactly the rate of growth of the information transmitted with every extra photon sent from Alice to Bob. Although, in theory, one bit of information is only achieved asymptotically, when the number of photons transmitted is arbitrarily

large, we can clearly see that for all practical purposes, 9 or 10 photons are enough to distinguish between a bit 0 and a bit 1 with a very high probability.

Even though encoding in the entanglement domain is not as efficient as other methods (such as manipulating polarization or spin of a particle), the important property of spatial entanglement is that it leaves the door open for a second encoding that can be applied to the same particle. This ultimately means that spatial entanglement of any particles, not just photons, can be used as a general method for increasing the capacity of a quantum communication channel. For a concrete example, suppose that in Fig. 1, before each photon detector (horizontal or vertical), we place a polarizer beam splitter to distinguish between the base states characterizing a certain polarization basis (for example, horizontal/vertical polarization). A Mach–Zehnder interferometer enhanced with polarizer beam splitters in this manner is presented in Fig. 4 in the context of describing a quantum key distribution scheme using double encoding (both in the entanglement and polarization domains). In this way, we can transmit more than one bit of classical information for each photon traveling from source to destination.

In principle, this double encoding idea can be generalized to any particle that may be used as a physical embodiment for a qubit, allowing that particle to carry more than just one bit of information. For example, if the physical implementation of a qubit is chosen to be an electron, we can encode $n + 1$ bits of information for each group of n electrons, by encoding one bit in the spin of each electron and another one collectively on the whole group by distinguishing between entanglement and non-entanglement. Of course, the Mach–Zehnder interferometer will have to be replaced in that case with an analogous experimental setup that allows an electron to interfere with itself [12].

Note that this variant of superimposing two different encodings on the same physical support (a photon) is different from both superdense coding [5,13] and some recent attempts to improve the efficiency of quantum key distribution schemes by combining encoding in the polarization domain with spatial encoding [1,20]. Superdense coding refers to a protocol that can transmit two classical bits of information by sending only one qubit from source to destination. The two important characteristics that make superdense coding different from our scheme are the assumption that the two parties share an entangled state to begin with, and secondly, the fact that the encoding is done in a single domain, which depends on the particular physical embodiment chosen for a qubit (polarization of a photon, spin of an electron, etc.). Thus, superdense coding achieves a channel capacity of two bits per qubit (or particle) using a single encoding domain, but at the expense of a previously shared entangled pair between the sender and the receiver. Our scheme does not achieve two bits of information transmitted for each particle traveling from source to destination, but also does not require any pair of entangled particles to be shared by the sender and the receiver as a prerequisite. Furthermore, our double-encoding scheme uses two different domains in order to encode information.

With respect to the recent proposals to improve efficiency of key agreement protocols through a better utilization of a photon, the double encoding is performed in separate domains: polarization and position, or, as the authors call them, *polarization and spatial-mode degrees of freedom*. However, unlike our scheme, their spatial encoding requires distinguishing between two different optical paths or ways that can be used by a photon to travel between the communicating parties. Figure 3 shows

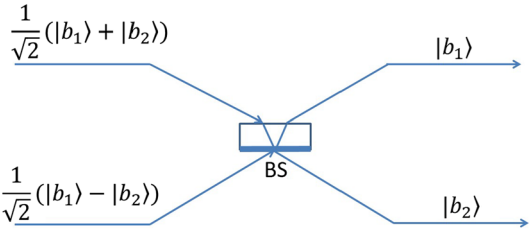

Fig. 3 Encoding a bit of information in the spatial-mode degree of freedom

the two non-orthogonal measuring bases that can be used for encoding in the spatial-mode degree of freedom. The beam splitter acts as a unitary operator that rotates basis $\{\frac{1}{\sqrt{2}}(|b_1\rangle + |b_2\rangle), \frac{1}{\sqrt{2}}(|b_1\rangle - |b_2\rangle)\}$ into basis $\{|b_1\rangle, |b_2\rangle\}$.

In a practical implementation, b_1 and b_2 may correspond to two different fiber optic cables and the receiving party has the choice of measuring the position of the incoming photon in one of the two bases by applying or not the beam splitter operator before placing photon detectors on the two possible physical paths. Therefore, if each path is considered a channel, then the amount of information transmitted per channel is still one bit. In contrast, our scheme requires only one path or channel connecting the source to the destination, as the photon always enters the Mach–Zehnder interferometer horizontally. Consequently, our double encoding scheme achieves a capacity higher than one classical bit of information per channel.

4 A QKD scheme using spatial entanglement as the encoding domain

In this section, we show in detail how spatial entanglement can be used for the purpose of establishing a secret key between two parties, Alice and Bob, without them ever having to meet. They are assumed to have at their disposal both a quantum and a classical communication channel. For the purpose of our scheme, the quantum channel may be unidirectional, allowing Alice to send an arbitrary number of photons to Bob. The classical channel must be bidirectional and is used by the two parties to check for eavesdropping and for key reconciliation. Both the quantum and the classical channel are assumed to be public, and consequently open to eavesdropping, but the classical channel needs to be authenticated, so that each party has the certainty of "talking" to the other participant to the protocol.

The scheme consists of the following steps:

1. Alice generates a random binary sequence $x_0, x_1, x_2, \ldots, x_N$. For each bit x_i, $i = 1, \ldots, N$, Alice prepares and sends to Bob a group of n photons. If the bit is zero, each photon sent is part of a pair of spatially entangled photons $a_{ij}b_{ij}$, where $i = 1 \ldots N$ and $j = 1 \ldots n$. Photon b_{ij} is sent over to Bob through the quantum channel, while its pair a_{ij} remains in Alice's possession and is being directed through a Mach–Zehnder interferometer. In the other case, when the bit is one, each photon in the group is a "regular," unentangled photon.
2. As Bob receives each photon sent by Alice, he also feeds them to a Mach–Zehnder interferometer and records which way each photon exited the interferometer.

3. Eavesdropping verification and key reconciliation:
Once all $N \cdot n$ photons have been received and processed by Bob, Alice and Bob together decide on a fraction f of the entangled photons to be checked for correlations in the path taken to exit the corresponding interferometer. If the photons have not been "meddled with" while in transit from Alice to Bob, the output recorded by Bob should match exactly the label recorded by Alice, for two photons belonging to the same pair. If the number of mismatches detected in the verification phase is above a certain agreed upon threshold, the protocol is abandoned due to the presence of an eavesdropper. Otherwise, the remaining $(1 - f)N$ photons are used to generate the secret key through specific distillation procedures [2] aimed at resolving possible remaining differences in the key due to low levels of eavesdropping and/or misclassifications of an entangled photon as a regular one (such an event may still happen with probability $1/2^n$).

4.1 Man-in-the-middle attack

An eavesdropper on the quantum channel, henceforth referred to as Eve, aims to gain knowledge about the information encoded in the passing photons. She can do so by "measuring" their entangled/non-entangled state through the use of a Mach–Zehnder interferometer, just as if she were Bob. If a photon is part of a group that carries a one (that is, a non-entangled photon), then it will exit the measurement apparatus horizontally and Eve can pass it along to Bob. In this case, she can learn the value encoded by group to which the photon belongs without being detected.

On the other hand, if the photon is part of a group that encodes a zero, then it will be detected either by D_1 or D_2 with equal probability. As it is customary to assume that an eavesdropper has unlimited resources (computationally and otherwise), we can adopt as a working hypothesis the fact that Eve's measurements are non-destructive, in the sense that a photon detected by a certain photon detector is not absorbed and it can be further manipulated in any other way Eve sees fit.

Which particular detector registers a click coincides with the output recorded by Alice for her photon a_{ij}, since the two are entangled. But now, regardless of whether Eve forwards to Bob the same photon she intercepted and measured, or she sends to Bob a "new" photon generated by her, when Bob passes the photon he receives through his interferometer, there will be no consistent correlation between the outcome he obtains and the outcome recorded by Alice. This is due to the fact that the Eve's Mach–Zehnder interferometer acts as a measurement device and breaks down the entanglement between a_{ij} and b_{ij} such that a second application of the interferometer (performed by Bob) yields no correlation between the output obtained by Bob and the output observed by Alice for its pair. Consequently, for each entangled photon b_{ij} sent by Alice and intercepted by Eve, there is a nonzero probability of detecting the disturbance induced by the eavesdropping act.

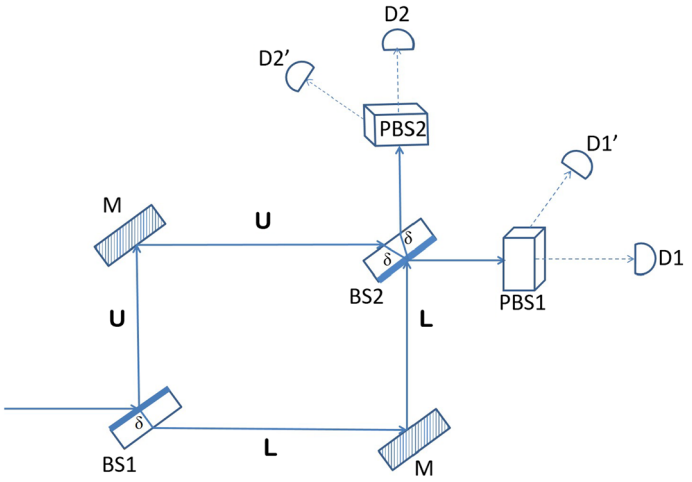

Fig. 4 Mach–Zehnder interferometer enhanced with polarizer beam splitters to measure the polarization of any photon exiting the interferometer

4.2 Extension to double encoding

The quantum key distribution protocol described above offers an example of how encoding information in the entanglement domain can be exploited for the benefit of secure quantum protocols. Compared with other quantum key distribution schemes, our proposal lacks efficiency, in the sense that it requires several photons in order to transmit one bit. The higher the number of photons in a group, the higher the confidence in the received bit. In practice, groups of nine or ten photons ensure almost certainty in obtaining the correct value of the bit they encode.

If encoding information in the entanglement domain may not seem very attractive on its own, due to this efficiency reason, it certainly is very appealing as a secondary encoding method, when combined with existing protocols that use an efficient encoding technique. It could be the case, for example, of the BB84 protocol [3] using the polarization degree of freedom of a photon to encode information, augmented with encoding supplemental information into the entanglement domain. This means that each photon traveling from Alice to Bob carries one bit of information encoded as a definite polarization state (which can be rectilinear or diagonal) plus some amount of extra information as part of a group in which every photon is an entangled one or every photon is unentangled.

At the other end, Bob has to use a modification of the Mach–Zehnder interferometer from Fig. 1 in which the photon detectors D_1 and D_2 are replaced with two devices that can measure the polarization of any photon exiting horizontally or vertically. Such a device is usually a polarizer beam splitter (made up of a doubly refracting calcite crystal) that can direct the photon along two different paths according to its polarization and then the presence of a photon along a particular path is detected with the help of photon detectors (see Fig. 4).

Any disturbances caused by an eavesdropper in the entanglement domain are detected using the procedure described in the previous section, while changes in the polarization state induced by Eve's actions are dealt with according to the steps detailed in the original BB84 protocol. In this way, the total amount of information transmitted can be augmented with an additional bit for every group of nine or ten photons, or whatever value of n Alice and Bob choose to work with. In a similar way, the entanglement domain can be combined with other degrees of freedom beside photon polarization (such as spin of a particle, for example) or even with multiple domains.

5 Entanglement domain, quantum bit commitment and superluminal communication

Having touched on possible applications of coding in the spatial entanglement domain, we close our exposition with the point that our scheme to distinguish an entangled photon from a non-entangled one cannot lead to an unconditionally secure quantum bit commitment (QBC) protocol, although apparently, such an ability should overcome the impossibility theorem for the existence of an unconditionally secure QBC scheme [14].

In a typical QBC protocol, Alice uses a key k_i of her choice to encode a bit value (0 or 1) into the state of a certain quantum system that is passed over to Bob. Bob should not be able to learn the value of the encoded bit until Alice provides him with the encoding key k_i at the decommit phase. As it was proved in [14], the very condition that prevents Bob from learning prematurely the bit value Alice has commited to, allows her to change her commitment in the decommit phase. However, in order to keep all her options open, she has to resort to *entanglement* between the qubits in her own quantum register and the qubits encoding the bit value and given to Bob.

To illustrate the point on a simple and concrete example, let us focus on the very first QBC protocol, described in the seminal BB84 paper [3]. Alice randomly generates a binary string of length n (which plays the role of the encoding key k_i) and encodes each bit from the string in the polarization state of a photon. She uses the horizontal/vertical polarization basis $\{|H\rangle, |V\rangle\}$ if she commits to zero and the diagonal basis $\{\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$ in case she commits to one. Since Bob has no knowledge of the binary string used as a key, he cannot distinguish between a photon with a horizontal/vertical polarization or a diagonal one. Alice also cannot change the polarization of the photons, once they have been passed over to Bob, so the protocol is secure with respect to both sides.

A dishonest Alice can cheat if instead of following the protocol as described above, she prepares n pairs of entangled photons in the state $\frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle)$, keeps one photon in each pair for herself and sends the others to Bob. In this way, at the time of revealing her commitment, she just has to measure the photons left in her possession in the horizontal/vertical basis for a commitment to zero, respectively, in the diagonal basis for a commitment to one. Bob remains ignorant of this cheating strategy since he cannot distinguish between an entangled photon and a non-entangled photon prepared either in the $\{|H\rangle, |V\rangle\}$ basis or in the $\{\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$ basis.

The ability to distinguish between entanglement and non-entanglement, as described in this paper, still does not help Bob's cause. In the first place, the *hiding* property of bit commitment requires that Bob should not be able to extract any information about the commitment from the quantum state of the photons received from Alice. This is ensured by using two complementary bases for encoding: horizontal/vertical and diagonal, both in the polarization domain. If the scheme described in our paper is to be applied to designing a QBC protocol, we would need a second encoding base, complementary to the $\{entangled(|E\rangle), non-entangled(|N\rangle)\}$ one. But this entails base vectors that would be superpositions of a photon being at the same time entangled and not entangled. It is not clear if something like this can exist from a theoretical point of view, let alone a practical realization. Furthermore, the entanglement used by Alice in her cheating strategy, namely $\frac{1}{\sqrt{2}}(|E\rangle|E\rangle + |N\rangle|N\rangle)$ would be some sort of *meta-entanglement* since it would entangle together qubits (realized as photons) that are already encoding information in the spatial entanglement domain.

Finally, let us point to the fact that being able to distinguish between a photon entangled in the polarization domain and one that is prepared in the $\{|H\rangle, |V\rangle\}$ basis or the $\{\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$ basis would open the way for faster-than-light communication. Imagine a scenario similar to what happens in her cheating strategy, in which Alice generates entangled pairs of photons in the state $\frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle)$ and sends one photon from each pair over to Bob. Just before Bob receives such a photon, Alice could decide to measure its counterpart (left in her possession) in one of the two complementary polarization bases. This act of measurement would instantaneously affect the quantum state of the photon en route to Bob, forcing it to coincide with whatever Alice has measured: $|H\rangle$ or $|V\rangle$, if the measurement was performed in the horizontal/vertical basis, respectively, $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ or $\frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$, for a diagonal polarization measurement. And if Bob would have the ability to detect the difference between a polarization entangled photon and a non-entangled photon whose polarization state is one of the four base vectors, he would be able to receive information from Alice instantaneously over arbitrary large distances. However, since such a distinguishability problem is unsolvable, faster-than-light communication as well as unconditional quantum bit commitment remain both unattainable.

6 Conclusions

Entanglement is rightfully perceived as the most counterintuitive manifestation of the physical theory of quantum mechanics and harnessed accordingly, as a veritable physical resource, to give rise to equally surprising applications, like teleportation [4,7,9] or superdense coding [5,13]. In quantum cryptography, entanglement has been used on both sides of the barricade, either to help communicating parties to establish a secret key or to allow dishonest participants to cheat the requirements of some cryptographic primitive like bit commitment [19]. In all its different usages, entanglement was never contemplated as a degree of freedom in its own right, one that can be used to encode information and therefore effectively serve as the physical embodiment of a classical bit.

We have shown in this paper how entanglement can be used as a vehicle to encode and transmit information and how this information can be extracted through photon interferometry. Although the techniques described herein cannot be used to prevent entanglement-based attacks by distinguishing between entangled and non-entangled states, as explained in the previous section, encoding in the entanglement domain can be used as a building block to design cryptographic protocols, either on its own or, most likely, in combination with other degrees of freedom in order to enhance the security and/or efficiency of these protocols. We envisage that exploiting entanglement as a degree of freedom that allows for extra room to encode information will prove to be a useful tool for researchers to further advance the field of quantum cryptography.

References

1. Abulkasim, H., Farouk, A., Alsuqaih, H., Hamdan, W., Hamad, S., Ghose, S.: Improving the security of quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom. Quantum Inf. Process. **17**(11), 316 (2018). https://doi.org/10.1007/s11128-018-2091-7
2. Assche, G.V.: Quantum Cryptography and Secret-Key Distillation. Cambridge University Press, Cambridge (2006)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE, New York (1984), Bangalore, India December (1984)
4. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.: Teleporting an unknown quantum state via dual classical and EPR channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)
5. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. Phys. Rev. Lett. **69**(20), 2881–2884 (1992)
6. Born, M., Wolf, E.: Principles of Optics, 7th (expanded) edition. Cambridge University Press, Cambridge (1999)
7. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature **390**(6660), 575–579 (1997)
8. Brown, J.: The Quest for the Quantum Computer, Touchstone edn. Simon & Schuster, New York (2001)
9. Furusawa, A., Sørensen, J.L., Braunstein, S.L., Fuchs, C.A., Kimble, H.J., Polzik, E.S.: Unconditional quantum teleportation. Science **282**, 706–709 (1998)
10. Horgan, J.: Quantum philosophy. Sci. Am. **267**(1), 94–105 (1992)
11. Howell, J.C., Bennink, R.S., Bentley, S.J., Boyd, R.W.: Realization of the Einstein–Podolsky–Rosen paradox using momentum- and position-entangled photons from spontaneous parametric down conversion. Phys. Rev. Lett. **92**, 210403 (2004)
12. Ji, Y., Chung, Y., Sprinzak, D., Heiblum, M., Mahalu, D., Shtrikman, H.: An electronic Mach–Zehnder interferometer. Nature **422**, 415–418 (2003). https://doi.org/10.1038/nature01503
13. Mattle, K., Weinfurter, H., Kwiat, P.G., Zeilinger, A.: Dense coding in experimental quantum communication. Phys. Rev. Lett. **76**(25), 4656–4659 (1996)
14. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414–3417 (1997)
15. Nape, I., Otte, E., Vallés, A., Rosales-Guzmán, C., Cardano, F., Denz, C., Forbes, A.: Self-healing high-dimensional quantum key distribution using hybrid spin-orbit bessel states. Opt. Express **26**(21), 26946–26960 (2018)
16. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2010)
17. Pan, J.W., Chen, Z.B., Lu, C.Y., Weinfurter, H., Zeilinger, A., Żukowski, M.: Multiphoton entanglement and interferometry. Rev. Mod. Phys. **84**, 777–838 (2012)
18. Sit, A., Fickler, R., Alsaiari, F., Bouchard, F., Larocque, H., Gregg, P., Yan, L., Boyd, R.W., Ramachandran, S., Karimi, E.: Quantum cryptography with structured photons through a vortex fiber. Opt. Lett. **43**(17), 4108–4111 (2018)

19. Spekkens, R.W., Rudolph, T.: Degrees of concealment and bindingness in quantum bit commitment protocols. Phys. Rev. Lett. A **65**, 012310 (2002)
20. Wang, L., Ma, W.: Quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom. Quantum Inf. Process. **16**(5), 1–15 (2017). https://doi.org/10.1007/s11128-017-1576-0